193 Southdown Road
Edgewater, MD 21037
grcotter@comcast.net

September 14, 2020

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Dear Ms. Bose,

Attached, please find my 4th Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000, all Related to Critical Infrastructure Reliability Standards.

Respectfully,

/s/

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

4th Motion to Intervene in Dockets)	**(Docket No. EL20-46-000**
Related to Critical Infrastructure)	**(Docket No. AD20-19-000**
Reliability Standards)	**(Docket No. RM20-12-000**
	(Docket No. RM18-20-000

Introduction

Previous Motions to intervene in the cited dockets provided evidence that the implementation of Section 215 EPA of 2005 was deceptively minimizing actual Cybersecurity protections for the Bulk Power System, commonly referred to as the Bulk Electric System, BES. This 4th Motion to Intervene adds supporting evidence of exclusion of "Real-Time Power Flow Operations" from CIP protections, despite specific inclusion of BES operations in the provisions of Section 215, EPA 2005.

Multiple audits of NERC Registered Entities in Reliability Regions add evidence to the conclusion stated in this filer's 3rd Motion to Intervene[1] in the foregoing dockets, viz:

"The conclusion is therefore inescapable, this audit and assessment (ie., LIPA) not only lacked linkages to Critical Infrastructure Protection (CIP) standards but rigorously avoided any non-CIP Reliability Standard related to "Real-Time Operational Power Flows".

Discussion

Audits of utilities for compliance with industry ***non-CIP*** Reliability Standards are common under the CMEP program, undergoing review by NERC's Board of Trustees before forwarding to FERC for approval. Standards linked directly to Real-time Operational Power Flows are, however, not included, given the apparent prohibition on such functions. This must be carefully identified in advance of the audit and, in fact, would evidently rule out audits of Registered Entities that primarily operate in such venues. Examples would be certain ISOs and RTOs, such as PJM, that function in several "real-time" roles such as Transmission Operations, Balancing Authorities, BAs. And predictably, audits of REs primarily managing real-time operations will not be found in the NERC multi-year data base. The exclusion from cybersecurity standards cannot be justified under

[1]3rd Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000, August 20, 2020

any reasonable interpretation of Section 215 of EPA 2005 and thus is never openly discussed in any compliance audit, CIP or non-CIP. And it probably accounts for NERC's ongoing pressure on FERC to make all compliance audits, non-public.

Given the decade-long deception on the extremely limited extent of cybersecurity protection for the Bulk Power System, is FERC justified in examining funding alternatives for utilities' voluntary cybersecurity costs?[2] Not without full disclosure to the Congress and the public of the real cybersecurity resiliency of the BES. Filings from state PUCs on this docket reflect concerns for open-ended utility options that would impact rate payers. These filings also suggest state PUCs are in the dark on the level of cybersecurity protection already afforded the BES, or more properly the level of deception being practiced by NERC and FERC. To the latter's credit, its insistence in FERC Order no. 866[3] that NERC and the industry provide protection for not just data repositories but also for the communications and networks feeding such data into control centers. However, and significantly, FERC failed to provide a deadline for compliance, in Order no. 866.

California ISO non-CIP Compliance Audit[4]

From the audit:

"CISO is a nonprofit public benefit corporation organized under the laws of the State of California. CISO is the largest of 38 Balancing Authorities in the Western Interconnection, handling an estimated 35 percent of the electric load in the west. CISO does not own any Transmission Lines but CISO is responsible for monitoring and operating approximately 26,000 miles of Transmission Lines."

"CISO acts as a traffic controller by routing power, maximizing the use of the Transmission system and generation resources, and oversees the maintenance of lines as CISO is the final authority responsible for granting outages to these lines for maintenance. Additionally, CISO is responsible for determining SOLs and IROLs for these transmission lines."[5]

"CISO has the responsibility to coordinate system restoration activities with Participating Transmission Owners (PTOs). CISO is responsible for balancing 46,625 MW of load in its BA footprint. As a TSP, CISO has the capacity to deliver 68,095 MW of Real Power and operates and monitors a total of 13 transfer paths within its footprint."

It was therefore a surprise to find a ***non-CIP*** compliance audit on this ISO whose functions are almost entirely "real-time operations". It covered the period August 11, 2015 – August 28, 2018 and may have been necessary to the transition of compliance authority from Peak Reliability to the WECC, although Peak was still listed as the Reliability Coordinator in this audit. The ***non-CIP*** Standards within scope for this audit are shown in Table 2, below. Note that all but TPL

[2] CYBERSECURITY INCENTIVES POLICY WHITE PAPER June 18, 2020, Docket No. AD20-19-000

[3] [Docket No. RM18-20-000; ORDER NO. 866] Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security –Communications between Control Centers (Issued January 23, 2020)

[4] WECC Compliance Audit, California Independent System Operator NCR05048 Report, February 7, 2019

[5] SOLs = System Operating Limits IROLs = Interconnection Reliability Operating Limits

planning standards have real-time significance. Curiously, the audit text strongly suggests that some aspects of these standards were actually audited by the WECC. However, any in-depth examination would have required discussion with many of the over 100 So. California utilities listed as Registered Entities in this audit, an implausible likelihood considering the audit dates were limited to December 3-7, 2018.

Table 2: Compliance Audit Scope

Registered Function	Standards	Requirement(s)
BA	BAL-001-2	R2
BA	BAL-004-WECC-2	R3
BA	BAL-005-0.2b	R8
BA, TOP	COM-002-4	R2
BA, TOP	EOP-008-1	R6
TOP	EOP-011-1	R1
BA, TOP	IRO-017-1	R2
PA	PRC-023-4	R6
TOP	TOP-001-4	R10
TOP	TOP-001-4	R13
TOP	TOP-001-4	R14
BA	TOP-001-4	R23
BA	TOP-001-4	R24
TOP	TOP-002-4	R1
PA	TPL-001-4	R1

Table 2: Compliance Audit Scope

Registered Function	Standards	Requirement(s)
PA	TPL-001-4	R2 (R2.1.4, R2.1.5, R2.3, R2.8)
PA	TPL-001-4	R5
PA	TPL-001-4	R6
TOP	VAR-001-4.2	R2
TOP	VAR-001-4.2	R3

The team did not expand the scope of the Compliance Audit beyond what was stated in the notification package.

The team reduced the scope of the Compliance Audit from what was stated in the notification package.

Table 2b: Compliance Audit Scope (Reduced)

Registered Function	Standards	Requirement(s)
BA	BAL-005-0.2b	R7
BA	BAL-005-0.2b	R15

Table 2 above shows the "theoretical" extent of ***non-CIP*** Reliability Standards involved in real-time operational flows across the BES and that would be consistent with the actual

suppression of these standards in the NPCC ***non-CIP*** compliance audit of the Long Island Power Authority illustrated in this filer's 3rd Motion to Intervene[6] in these dockets. However, for this CISO audit, listing such standards was unnecessary or redundant, given the WECC "Reduced Audit Scope" listed in Table 2B, above.

Comment: Table 2B might just as well be labeled "Negated Audit Scope". The obvious conclusion is that, for whatever reasons this audit was initiated, there was never any intention to document the CISO ***non-CIP*** compliance record for "Real-time Power Flow Operations". Citing a retired Standard BAL-005-0 2b was simply cover for closing the audit. The alternative was to explain the purpose for the audit in the first place. But what this incident reveals, is further confirmation that the entire NERC Reliability Standards process does not permit any interference in "Real Time Power Flow Operations". Cybersecurity risks were not allowed to take precedence over that industry principle. However, putting utility "Real-Time Power Flow Operations" off-limits to any BES-wide compliance audits creates a gap in evolution of Reliability Standards, an increasingly widening gap. Reliability engineering standards are getting dangerously out of synch with utilities' technology upgrades undercutting functioning of Balancing Authorities, seriously delaying resolution of Reliability Area metric variations (e.g., frequency/phase) and preventing application of effective cybersecurity controls to operational systems. Yes, national risks to critical infrastructures, including the nation's election systems and many important national security facilities, were intentionally discounted in the process.

Systemic Flaws in Recent FERC Actions

The foregoing series of events goes from the weird to the ridiculous to the sublime when the chronology is examined. Standard BAL 005-0.2b was retired by FERC Order no. 836 September 20, 2017, ***3 months before completion of this audit and fully 6 months before the audit was filed*** on February 7, 2019. For the Reduced Audit Scope in Table 2B above, Requirement R 7 cannot be traced through the nearly continuous modifications of NERC Reliability Standards but Requirement R15 stands out clearly in FERC Order no. 836 involving Balancing Authority Control, Inadvertent Interchange, and Facility Interconnection Reliability Standards. In its order FERC ultimately yielded to NERC and utility pressures to accept multiple safeguards for absence of control center back up power sources required by R15 in the retiring BAL-005-0.2b.

As revealed in this filing, **non-CIP** Reliability Standards show no linkages to CIP Standards. Separate compliance audits assess utilities conformance to those standards. Further, "Real-time Operational Power Flows" actually appear to be exempt from **non-CIP** RE compliance audits. By what logic then is NERC and the industry permitted to cite those standards in support of vulnerabilities in CIP Standards? Thus, the addition of Docket no. RM18-20-000 to this Motion to

[6] 3rd Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000, August 20, 2020

Intervene. The issuance of Order No. 866 Final Rule leaves unaddressed, a dispute tracing back to Order No. 822, an order perpetuating a major vulnerability from the initiation of CIP Standards; i.e., exclusion of communications and networks from CIP Standards in CIP-002. Indeed, in Order no. 866, FERC essentially admits that the exclusion cannot apply to communications/networks and their data flows between control centers. NERC and its supporters again extensively cite elements of **non-CIP** Reliability Standards in an unsuccessful effort to convince FERC to drop the issue, as a continuing vulnerability of CIP-012-1. However, it remains an open task for the ERO. No deadline is specified but media concludes that it must be fixed by the 2022 implementation date for CIP-012-1.

However, FERC should never have agreed to waive the need to identify the data involved, i.e, "***43. With this understanding, we are satisfied that the data protected under Reliability Standard CIP-012-1 is the same data identified under Reliability Standards TOP-003-3 and IRO-010-2."*** Neither of those **non-CIP** Relibility Standards were included in the CISO audit documented in this filing and neither address data flows that are the key linkages to the Synchrophasor modernization explosion and other modernization initiatives. ***See yellow highlighted text above and the attachment to this filing. Further, exclusion of such standards from non-CIP compliance audits makes a nonsense of the association with CIP-012-1. As written, CIP 012-1 will not reduce control center vulnerabilities. On the contrary, it provides the nation's adversaries pathway directions for attacks.*** But FERC Order no. 866 does help to illuminate the problem. Hopefully, this and previous filings will inform the public and the Congress of serious ethical if not legal, issues that must be addressed.

Conclusion

This filer's most recent White Paper[7] was addressed, inter alia, to the Secretary, Department of Energy with a recommendation that the DoE/FERC IG investigate the decade long deception and possible violation of the Energy Policy Act, 2005 Section 215. Previous Motions to Intervene on these dockets were attached. Chairman Chatterjee was a recipient of those reports.

FERC can continue to ignore critiques of the implementation of Section 215 but would be well-advised to change course:

1. The FERC Staff "White Paper" on incentives for Utilities voluntary cybersecurity expenses should be shelved. Until and unless FERC faces up to the deception of the current CIP charade, its credibility as a balancing force between the industry and the public is void.
2. Under Section 215 and Section 219 authorizations, freeze CIP Standards actions.

[7] "Security in the North American Grid – Hidden Cybersecurity Vulnerabilities", A White Paper, August 20, 2020

3. Task NERC to immediately develop modifications to its Reliability Standards to incorporate Syncrophasor and other modernization technologies and address BES real-time operations.[8]
4. Under the assumption that the Congressional Cyberspace Solarium Commission recommendation for a National Deterrence Policy will be implemented, task NERC to develop a plan for transition of the BES, region-by-region, to NIST Standards.
5. CIP Standards can then be modified to address unique vulnerabilities or threats under NIST cybersecurity guidelines. That plan must, of course, protect ***non-CIP*** Reliability (engineering) Standards critical to operations of the North American Grid.

All this will take time, but it would eliminate most of the gaps in cybersecurity protections for both the BES and Distribution systems since non-BES utilities will follow the trend to adoption of NIST standards, state by state.

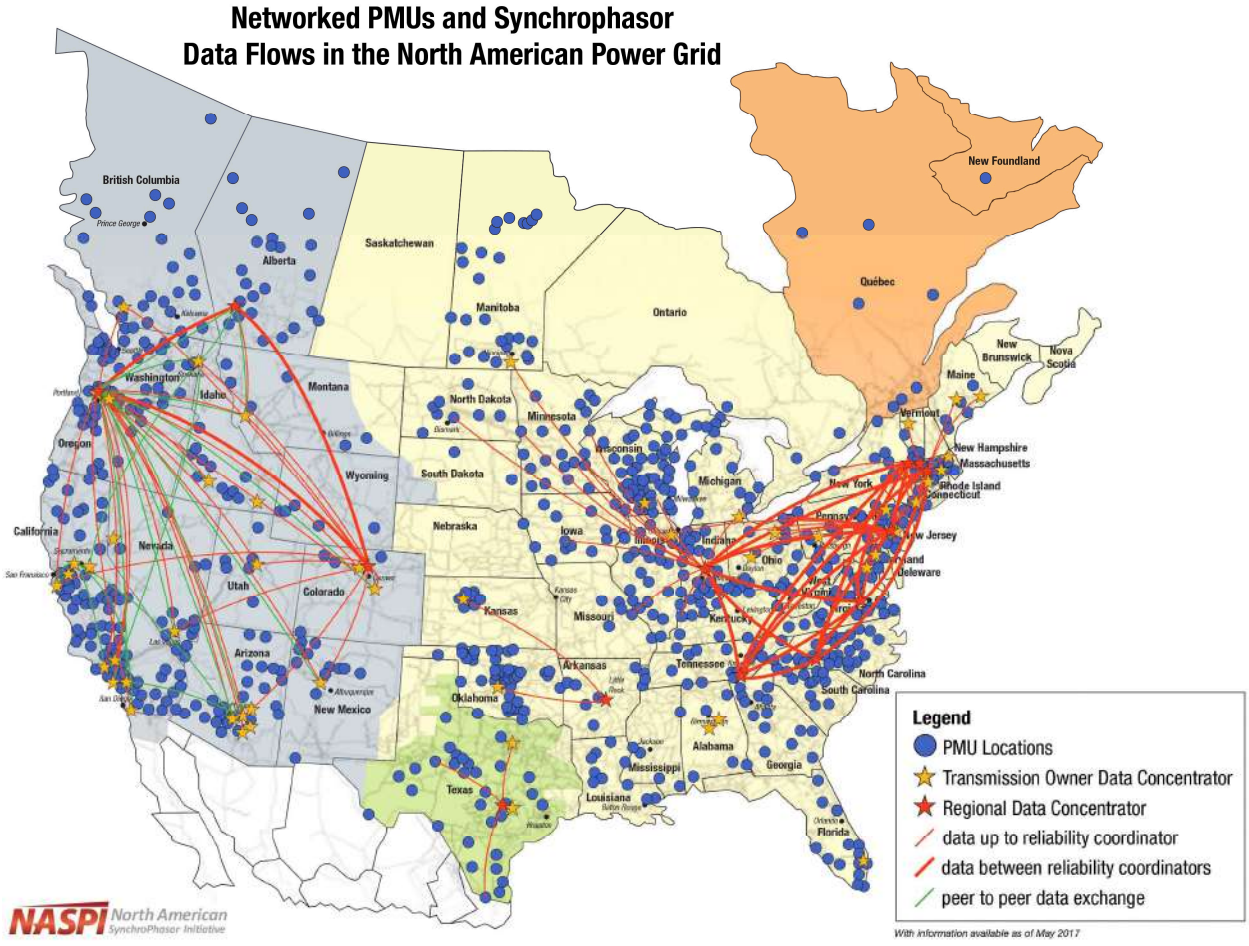
Respectfully Submitted,

George R. Cotter

[8] There is little doubt that the increased costs of the complexity of this distorted compliance process have been passed on to power users in tariffs.

Attachment to 4th Motion to Intervene

Note: Real-Time Data Flows involving Bulk Electric Systems are excluded from Compliance Audits for the California ISO Reliability Entities documented in this Report. This also probably applies to other BES Compliance Audits in other Regions.[9]



[9] See Long Island Power Authority **non-CIP** Compliance Audit documented in 3rd Motion to Intervene in these dockets

Document Content(s)